United States Department of Justice
Federal Bureau of Investigation

October 1, 2008 **FBI INDIANAPOLIS**
Immediate Release

LAW ENFORCEMENT UNRAVELS EXTORTION SCHEME AND PREVENTS LARGE SCALE IDENTITY FRAUD

Michael S. Welch, Special Agent in Charge of the Indianapolis Office of the Federal Bureau of Investigation (FBI); Steve Carter, Indiana Attorney General; and Chief Michael Spears, Indianapolis Metropolitan Police Department jointly announced today the arrest of Kevin Michael Stewart by the FBI Cyber Crime Task Force and the Safe Streets Task Force in Indianapolis, Indiana at 12:30 a.m. this morning.

Stewart is currently facing federal charges arising from the March 31, 2006 burglary of a computer server from the Indianapolis office of Medical Excess LLC, a member company of AIG. The server contained personally identifying and health care sensitive information for over 900,000 policy holders. Stewart is also accused of extorting AIG for $208,000 under a threat to release the data onto the Internet beginning on July 23, 2008. A criminal complaint has been filed with the U.S. District Court for the Southern District of Indiana alleging violations of the extortion statute, Title 18, U.S.C. § 875 and the newly enacted Title 18 U.S.C. § 1030(a)(7)(B) and (C), which make it a federal crime to commit extortion relating to unauthorized access of, or damage to, a protected computer system and/or to impair the confidentiality of information obtained from a protected computer. "Stewart is believed to be the first person in the United States to be charged under this new criminal statute, which is designed to address the theft of large data sets from organizations and the resulting consequences," commented Assistant U.S. Attorney Steven DeBrota.

"AIG reported this matter immediately to the FBI, and worked proactively and aggressively with the multi-agency task force to solve the burglary and prevent the disclosure of sensitive customer information," said SAC Welch. He went on to say, "The stakes are high when dealing with a threat of this nature, as significant damage to our citizens and our financial infrastructure can occur with a single keystroke."

"When a company as large as AIG is vulnerable, we know that all businesses are threatened by cyber crime," said Attorney General Steve Carter. "The world became a smaller place with the advent of the Internet and when individuals utilize the medium for criminal

purposes, there are virtually no barriers on the amount of damage that can occur. It takes coordination and specialization to effectively investigate and successfully prosecute cyber-related crimes."

The FBI Cyber Crime Task Force is a multi-agency investigative unit with members in the FBI Indianapolis Field Office, Merrillville Resident Agency, and Evansville Resident Agency. The mission of the task force is to protect Indiana's citizens by investigating and preventing high technology crime and neutralizing national security threats involving computer networks. This is accomplished by leveraging the resources and expertise of participating law enforcement agencies, Indiana's higher-education institutions, and members of the U.S. Intelligence Community.

Agencies participating in the task force include the Evansville Police Department, Federal Bureau of Investigation, the Indiana Attorney General's office, Indiana Department of Natural Resources, Indiana State Police, Indianapolis Metropolitan Police Department, United States Secret Service, and the Vanderburgh County Sheriff's Office. Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) and Department of Computer and Information Technology's Cyber Forensics Lab are special partners in the task force.

Contact: Special Agent Wendy A. Osborne, FBI Indianapolis, (317) 639-3301.